Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

REPLY COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Brian M. Josef
Assistant Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

Dated: July 14, 2017

TABLE OF CONTENTS

Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

REPLY COMMENTS OF CTIA

I. INTRODUCTION AND SUMMARY

The initial comments in this proceeding show that wireless providers, correctional institutions, and vendors share the same goal of preventing inmates' use of contraband wireless devices. The record shows that wireless providers have worked with contraband interdiction system ("CIS") providers to deploy managed access systems ("MASs") – leasing spectrum, addressing technical challenges and preventing interference, and even providing legal, regulatory, and other support to the correctional community.[1] MAS solutions have proven very effective at combatting the contraband device problem, enabling correctional facilities to prevent use of contraband wireless devices while not undermining the ability of legitimate, authorized subscribers to obtain service either on facility grounds or nearby.

The record also shows that additional efforts to advance CIS solutions demand a collaborative approach. Several commenters provide meaningful input on the development of a reasonable and lawful policy framework for Cell Detections Systems ("CDS") solutions. That framework should establish a cooperative process for wireless carriers, correctional facilities,

[1] Comments of AT&T at 4 (filed June 19, 2017); Comments of Verizon at 3 (filed June 19, 2017); Comments of T-Mobile at 3 (filed June 19, 2017).

and CIS providers to advance a meaningful, reasonable, and technology-neutral CDS solution. Other technologies, including jamming, beacon-based, quiet zone, or wireless network-provided, suffer from substantial legal or technical hurdles and have too many problems for the Commission to pursue.

II. THE RECORD IDENTIFIES KEY ASPECTS OF A SOUND FRAMEWORK FOR CELL DETECTION SOLUTIONS

The Further Notice[2] set forth a series of specific questions for how to advance a CDS policy framework – and commenters responded with clear, sound, and reasonable input for how to move forward.

A. The Commission Should Establish Clear Standards for a Qualified Request.

Commenters agree that it is critical for the Commission to adopt reasonable, workable definitions of CIS eligibility, a qualified request, and an authorized party to make requests, to provide clarity and certainty for CDS solutions and protect the continuing operation of authorized wireless devices.[3]

CIS Eligibility. Commenters urge the Commission to adopt performance standards for CIS systems, and determine the eligibility of each system, in order to ensure certain functionality and minimize the risk of disabling a non-contraband wireless device.[4] ShawnTech Communications, for example, urges the FCC to adopt a comprehensive certification process to protect legitimate wireless devices, which certain CDS solutions might otherwise seek to disable

[2] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 2336 (2017) ("Further Notice").

[3] Comments of ShawnTech Communications at 3 (filed June 19, 2017); T-Mobile Comments at 8; CTIA Comments at 5; Verizon Comments at 5; Comments of Prelude Communications at 5 (filed May 1, 2017).

[4] ShawnTech Comments at 3; CTIA Comments at 5; Verizon Comments at 5; Prelude Comments at 5.

due to generating "false positives."[5] Verizon notes that eligibility standards would "ensure that correctional facilities and their vendors deploy and operate their systems per the terms of their spectrum leases and lease agreements and test the reliability of any cell detection system."[6] T-Mobile proposes that the Commission maintain a list of certified CISs.[7] And CTIA notes that the Commission should ensure that the cell detection system provider regularly calibrates the system's operation to ensure accuracy even after device certification and solution validation.[8]

Source of Request. Several commenters also urge the Commission to require a court order that would mandate wireless providers to prevent use of an unauthorized wireless device detected by a CDS solution.[9] As AT&T observes, a court order-led process "can be explained with two words: accuracy and familiarity."[10] AT&T highlights the courts' requirement of sufficient evidence to ensure accuracy and notes that law enforcement and wireless providers are familiar with existing criminal and civil procedures.[11] Indeed, Verizon highlights that "a court's evidentiary standards compel the party seeking injunctive action to have a valid factual basis for the request; service providers already have procedures in place that can be adapted to handle requests such as these; and the service provider does not face criminal or civil liability for implementing the request."[12] And, as T-Mobile notes, this approach provides "the checks and

[5] ShawnTech Comments at 3.

[6] Verizon Comments at 5.

[7] T-Mobile Comments at 8.

[8] CTIA Comments at 5.

[9] CTIA Comments at 5-6; T-Mobile Comments at 5-9; Verizon Comments at 4-5; AT&T Comments at 13-14.

[10] AT&T Comments at 9.

[11] *Id.*

[12] Verizon Comments at 4.

balances traditionally imposed by the government when alleged illegal activity is suspected."[13]

In contrast, those commenters who are concerned the court order approach would delay the termination process do not address the importance of adopting a high standard for termination requests.[14] A court order would ensure due process, can occur without sacrificing speed and efficacy, and is used in other law enforcement contexts, such as subpoenas.

Should the Commission decide not to adopt the court order approach, then the FCC itself should direct wireless providers to prevent operation of a wireless device.[15] That way, wireless carriers will be acting at the direction of the Commission, which oversees the effectiveness of the CDS process.[16] The only reasonable alternative is that all requests come from a certified senior state official with oversight of the CIS operator.[17] The rules should not require wireless providers to respond to requests by non-sworn law enforcement officials, *e.g.*, a warden at a privately owned and operated correctional facility or from the CIS provider itself, as such an approach would not provide sufficient safeguards for the public or for wireless providers.[18]

Content of Request. CTIA agrees with Verizon that requests should have a standardized, common format.[19] Also, a qualifying request should include a device's IMSI, the correctional facility in which the device is operating, why the device has been determined to be contraband,

[13] T-Mobile Comments at 5.

[14] Comments of Cell Command at 15-16 (filed June 19, 2017); *see also* ShawnTech Comments at 1; Comments of the Florida Department of Corrections at 1 (filed June 19, 2017); Comments of Core Civic at 2 (filed June 19, 2017).

[15] *See* AT&T Comments at 9-10; CTIA Comments at 6.

[16] CTIA Comments at 6.

[17] AT&T Comments at 15-16; CTIA Comments at 6.

[18] AT&T Comments at 15; CTIA Comments at 6.

[19] Verizon Comments at 9.

and documentation demonstrating that the equipment and process used complies with the FCC's certification and validation procedures.[20]

B. The Commission Should Adopt a Reasonable Approach to Preventing Use of Contraband Wireless Devices.

The Commission should require CDS solutions to identify the IMSI associated with an unauthorized wireless device, and require the wireless provider to block use of that IMSI, thereby terminating service to the contraband wireless devices. A fully engaged CDS will allow correctional institutions to continuously sweep their facilities, so that any attempted use of multiple SIMs in a device will be thwarted as the CDS identifies the unauthorized IMSIs.

Several commenters explain that a broad mandate to fully disable contraband wireless devices, as opposed to simply terminating wireless service to them, is difficult to effectuate.[21] As Verizon makes clear, any such approach would be extremely complicated, requiring extensive development and collaboration by a number of players in the wireless ecosystem.[22] The ability to disable a device is tied to a user's account with the operating system, not the unique device identifiers available to the licensee.[23] Therefore, the operating system provider, such as iOS or Android, would have to disable the device, not the wireless provider.[24] And even once developed, this capability would not extend to many of the handsets in the market today because the ability to disable and re-enable handsets is "limited to certain smartphone models

[20] CTIA Comments at 6; *see also* T-Mobile Comments at 8.

[21] Verizon Comments at 8-9; AT&T Comments at 8; T-Mobile Comments at 2, n. 5.

[22] Verizon Comments at 8.

[23] *Id*.

[24] *Id*.

and not available for feature phones and other connected devices."[25] As T-Mobile states, it may not be technically feasible or economically viable to disable devices.[26] In addition, the FCC's proposed approach could enable third parties to disable devices (not device owners) and create cybersecurity risks. Rather, as described above, the FCC should require wireless providers to implement qualifying requests by blocking the use of the IMSI, thereby terminating service to the contraband wireless device.

C. Wireless Providers Should Fulfill the Request, and CIS Operators Should be Responsible for Monitoring for Network Developments.

Numerous commenters note that the role of wireless providers should be limited to carrying out the mandate to prevent use of the device on its network.[27] Wireless providers should not be required to provide notification to CIS operators of technical changes. Network changes are months or years in the making, and addition of new frequencies available for CMRS use are made public, providing CIS operators with ample time to modify their systems as necessary. Contrary to commenters such as CellBlox Acquisitions,[28] able and responsible CIS operators should have the capability to monitor and identify wireless provider network changes without the need for prior carrier notifications. Many do already and there is no gap.[29] Indeed, some lease arrangement agreements require the CIS operator to monitor for carrier network changes.[30] As Verizon explains, details such as notifications should be left to contractual

[25] *Id*. at 9.

[26] T-Mobile Comments at 2, n. 5.

[27] Verizon Comments at 10-11; T-Mobile Comments at 13; CTIA Comments at 7-8.

[28] Comments of CellBlox Acquisitions at 4-5 (filed June 19, 2017).

[29] *See, e.g.*, Verizon Comments at 11.

[30] *See, e.g.*, Verizon Comments at 10-11; CTIA Comments at 8.

arrangements between the parties.[31]

D. The Commission Should Foster Good-Faith Compliance Efforts and Provide Liability Protection.

As with MAS solutions, the wireless industry is ready to work with CDS vendors and correctional institutions to enable CDS systems that will prevent use of non-contraband wireless devices – but commenters widely agree that the unintentional termination of legitimate services could endanger the safety of the user.[32] It could also create disputes, potential liability, and harm to wireless providers' goodwill. Many of the steps identified above will help ensure that CDS solutions function properly and reduce the risk of directing wireless providers to prevent use of authorized wireless devices. Furthermore, the FCC should ensure that the CDS termination process is not subject to abuse or maleficence.

But the Commission should do more. The record shows support for the adoption of a safe harbor rule for wireless providers seeking to comply with the federal process for preventing the use of phones in correctional facilities.[33] Further, the Commission should provide liability protection for wireless providers that make good faith efforts to comply with the rules. As T-Mobile states, the Commission should "expressly state that CMRS carriers are not liable for any consequences resulting from the deployment of the technologies."[34] These steps would eliminate potential obstacles to robust participation by wireless carriers in efforts to protect the public.

---

[31] Verizon Comments at 10-11.

[32] *See, e.g.*, Verizon Comments at 2; AT&T Comments at 5; T-Mobile Comments at 2.

[33] *See* Prelude Comments at 10; CTIA Comments at 9.

[34] T-Mobile Comments at 12.

III. THE COMMISSION SHOULD REFRAIN FROM ADOPTING FRAMEWORKS FOR CERTAIN OTHER CIS SOLUTIONS

A. Jamming Technologies are Unlawful and Do Not Serve the Public Interest.

Despite the Commission's repeated and definitive statements that the proposed use of jamming technologies is against the law, a few parties in this proceeding press for the authorization of jammers in prisons.[35] Jamming by non-Federal entities is illegal under Section 333 of the Communications Act.[36] Nor is jamming a good policy solution. As the American Correctional Association observes, "[j]amming systems can be over-inclusive and interfere with legitimate wireless devices in the surrounding areas."[37] For these reasons, and reasons previously cited by CTIA in this proceeding,[38] the Commission should – again – reaffirm that jamming is illegal and will not be a realistic solution.

B. Beacon-Based Technologies are Ineffective, Burdensome and Would Require Substantial, Costly Changes Through Lengthy Processes.

The Commission also should reject arguments for beacon-based technologies. First, implementation of these systems would require all existing and future wireless devices to include specialized, proprietary software.[39] The Commission should not make an exception to its long-standing technology-neutral policy for such a sweeping technology mandate.[40] Second, any beacon-based approach would be costly, burdensome, and inefficient, with a lengthy

---

[35] *See, e.g.*, Comments of Global Tel*Link at 8 (filed June 19, 2017).

[36] 47 U.S.C. § 333.

[37] Comments of American Correctional Association at 4 (June 23, 2017).

[38] *See* Ex Parte of CTIA, GN Docket No. 13-111, at 2-3 (filed Mar. 15, 2017); Ex Parte of CTIA, GN Docket No. 13-111, at 2-3 (filed Mar. 16, 2017).

[39] CTIA Comments at 9.

[40] FCC, *Strategic Plan of the FCC*, https://www.fcc.gov/general/strategic-plan-fcc (last visited July 3, 2017) (stating that Commission "policies must promote technological neutrality").

implementation process. ShawnTech Communications and others recognize the cost would be heavily borne by device manufacturers.[41] Third, it would pose a threat to the safety of the public by blocking legitimate calls.[42] And there is nothing to prevent the misuse of beacon technologies by entities other than correctional facilities once software is installed on phones. For example, using the same technology, people or entities could install beacons unbeknownst to the public, *e.g.*, in a movie theater, office, sports arena, or any public gathering place, thereby preventing legitimate, and sometimes life-saving, cell phone use. Furthermore, it would effectively require the FCC to dictate a global standard, as such an approach would implicate standards work for devices and networks, as well as impacts to OS development. Finally, as T-Mobile points out, it would only encourage the importation of contraband phones without beaconing software.[43]

C. Quiet Zones Would Restrict Network Design and Affect Service Around Corrections Facilities.

The record showed general opposition to quiet zones. Verizon states that quiet zones "impose significant costs on licensees and adversely affect the reliability of service to consumers."[44] T-Mobile states that quiet zones are technically infeasible given that specific boundaries cannot be established given the propagation characteristics of radio frequencies.[45] Cell Command states, "jamming and geo-fencing also have the real potential to interfere with legitimate wireless devices operating within the range of the jamming system."[46] One

[41] *See, e.g.*, ShawnTech Comments at 5.

[42] CTIA Comments at 10.

[43] T-Mobile Comments at 19.

[44] Verizon Comments at 12.

[45] T-Mobile Comments at 16.

[46] Cell Command Comments at 11.

commenter argues that quiet zones would be workable for maximum security prisons that are not close to public access,[47] but as CTIA previously stated, even in those rural areas wireless service is often provided via higher power antennas on taller towers that cover great distances.[48] A network re-design to engineer new quiet zones could easily take rural consumers near correctional facilities out of service.[49] Further, because some correctional facilities are located near busy interstates, quiet zones could take travelers out of service.[50]

D. There is No Lawful Basis for the Commission to Require Wireless Providers to Develop and Implement Their Own CIS.

Finally, a mandate on wireless providers to adopt and implement new network-based solutions would not be not a reasonable or legally sound approach.[51] Verizon rightly states that a network-based solution would be dependent on the development of device-level capabilities that would take "years to implement and even longer to meaningfully limit the abuse of contraband handsets."[52] Further, CMRS carriers do not actively track precise customer location information and are prohibited from doing so without prior customer authorization under Section 222 of the Communications Act.[53] It is unclear whether the purpose of the proposed approach fits within the permitted exceptions to Section 222. And, as highlighted above in the beaconing context, this approach also would require the FCC to dictate a global standard. Finally, as Prelude Communications points out, non-compliant devices can be easily sourced from abroad creating

[47] Global Tel*Link Comments at 8.

[48] CTIA Comments at 10.

[49] CTIA Comments at 10; T-Mobile Comments at 16; Verizon Comments at 12.

[50] CTIA Comments at 11; T-Mobile Comments at 16.

[51] Verizon Comments at 13; CTIA Comments at 11-12.

[52] Verizon Comments at 13.

[53] CTIA Comments at 11-12 (citing 47 U.S.C. § 222(h)(1)).

an entirely different problem for correctional facilities.[54]

IV. CONCLUSION

CTIA is proud of the role its members have played in assisting correctional institutions and third party vendors in the fight against the use of unauthorized, contraband wireless devices. CTIA commends the Commission's actions to streamline that process and urges the Commission to embrace a cooperative process for wireless carriers, correctional facilities, and CIS providers to advance a meaningful, reasonable, and technology-neutral CDS solution.

Respectfully submitted,

/s/ Brian M. Josef

Brian M. Josef
Assistant Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

Dated: July 14, 2017

[54] *See generally* Prelude Comments at 2.